I. Amendments to the Specification

Please amend the specification by deleting or canceling the previous versions of these paragraphs and replacing them with the following versions of the paragraphs.

Page 9, lines 4-14:

If a certificate authority issues a certificate for an entity, the entity must provide a public key and some information about the entity. A software tool, such as specially equipped Web browsers, may digitally sign this information and send it to the certificate authority. The certificate authority might be a company like ~~VeriSign~~ VERISIGN that provides trusted third-party certificate authority services. The certificate authority will then generate the certificate and return it. The certificate may contain other information, such as dates during which the certificate is valid and a serial number. One part of the value provided by a certificate authority is to serve as a neutral and trusted introduction service, based in part on their verification requirements, which are openly published in their Certification Service Practices (CSP).

Page 13, lines 8-12:

In another exemplary embodiment, the callee software module 280 may use the certificate 260 and/or public keys contained within the caller software module ~~110~~ 210 to both ~~to~~ verify and authenticate the caller software module 210. In this case, the caller software module 210 is digitally signed with a private key, and this signature is placed into the caller software module 210.

Page 13, lines 8-12:

Fig. 3 is a block diagram of an embodiment of the certificates relating to the invoked class according to the invention of Fig. 2. In this case, a plurality of certificates 320a-n is provided in the calling class 310. When implementing the invention in ~~Java,~~ JAVA, the certificates are "obfuscated", or kept from view. In this manner, a preliminary level of security may be maintained for these certificates.

Page 14, lines 14-17:

Fig. 4 is a block diagram of a method by which the invention of Fig. 2 may be implemented. In a block 410, the calling class determines that it needs to instantiate an invoked class. The calling class obtains the codebase of the invoked class in a block ~~470.~~ 415.

Page 15, lines 13-16:

However, if the verification, authentication, and/or authorization steps are successful, the invoked class constructor passes to successful completion in a block ~~480.~~ 470. This allows the invoked class and the calling class to operate and interact in a normal manner.

Page 15, lines 17-22:

In an exemplary implementation, the calling class and invoked class are implemented in ~~Java,~~ JAVA, and the digital signatures are those of the particular .jar file of each class, respectively. In this case, the schema may use the digital signature mechanisms provided by the ~~Java Runtime Environment~~ JAVA RUNTIME ENVIRONMENT (JRE). The JRE includes ~~Java Cryptography Architecture~~ JAVA CRYPTOGRAPHY ARCHITECTURE (JCA), which in turn provides implementation for many different signature algorithms.